ASSIGNMENT 2

ITRI 615

Enrico Dreyer
31210783

Table of Contents

Introduction

This report will cover the protection of Windows XP and how it achieves or implements separation, memory and address protection, file protection, user authentication, policies, trust, and assurance. This report will also address open-source operating systems and open-source software, as well as how they contributed in terms of improving operating system security.

Windows XP

Microsoft Windows XP was released in 2001, this was a year after the release of Microsoft Windows 2000. This operating system was meant to fix the cycle that Microsoft had of releasing separate systems for enterprises and consumers, and have a system that everyone can use (Goretsky, 2014). As of April 2014, around 30% of customers' desktop computers had Windows XP installed (Goretsky, 2014).

Separation

For systems like Windows XP that have to maintain separation of information, that perform at different levels of classification, a high assurance of security design is required (Staff, 2006). According to BrainKart (2019) there are different kinds of separation:

Physical separation – this is when two different hardware facilities uses two different processes. For example, non-sensitive operations can be run on a public system and sensitive tasks can be performed on a different computing system.

Temporal separation – this occurs when processes are run at different times. For example, you run non-sensitive processes between 08:00 and 16:00, then run sensitive data between 17:00 and 18:00.

Logical separation – this is when a process of one user, such as reference monitoring, is done separate from another user.

Memory and address protection

This includes protection to the memory that the operating system and the user processes uses. The challenging part of multi-programming systems is the prevention of one program from affecting the programs and data of other users in the memory space (Bagwe, 2016).

According to Bagwe (2016) there are different methods that can be used to protect memory and addresses:

Fence – this is an address, that processes of a user can not cross. The operating system can only operate on one side of this fence, the other side is restricted. This fence can be static, in that case the fence address is fixed. Alternative to this is a dynamic fence, what can be implemented by using a fence register that can specify a "current fence address".

Base and bounds registers – this protection is used in multi-user environments. This is where one user program has to be protected from another user. Each user has a bound register, called the upper address, as well as a base register, called the lower address. This approach assumes that the user or the process space is proximate in memory.

Tagging – this is used to protect individual addresses. With this method, every "machine memory word" has an extra bit to identify what access rights the word has. Privileged instructions are used to set the access bits. With the exception of significant overhead, it is fine-grained protection.

Segmentation – this is when memory is divided into logical units, for example dividing individual data or procedures in one array. After the division, access control that is appropriate to that segment can be enforced. A benefit to this is that any segment can be put into any memory location when given the location, considering the location is big enough to store it. Windows XP as the operating system needs to track all of the segments.

Paging – this method gets rid of the downsides of segmentation. All of the segments are a fixed size, this is then called paging, and the memory that is divided is called the page frames. The advantage of this method is that there is no fragmentation, and no variable size to be concerned about. Paging heavily increases efficiency.

File protection

Windows File Protection (WFP)

According to Microsoft (2020) their windows file protection is there to prevent programs to replace windows systems files that are crucial to functionality. Programs should not be able to alter or remove these files because they are being used by the operating system. This prevents the operating system and necessary programs from crashing or being used for malicious activity.

The file protection uses catalog files and file signatures that are made by code signing, and verify the protected system files to make sure that the correct Microsoft versions are being used (Microsoft, 2020). Only the following mechanisms can be used to replace protected system files:

- Windows Service Pack installation (Update.exe)
- Hotfixes installed (Hotfix.exe or Update.exe)
- Operating system upgrades (Winnt32.exe)
- Windows Updates

If a different program is used and does not pass the verification, the windows file protection will use and replace the program to the original file.

How it works

The WFP uses two mechanisms for the protection of system files. One of the mechanisms run on the background and is triggered when the WFP gets a notification of a directory change for a file. After the notification, the WFP pinpoints the file that was changed. When the file is protected by the WFP, the WFP compares the file signature that is located in the catalog file, to determine if the file is indeed the correct version.

The other type of mechanism is a feature that is provided by the System File Checker tool. After the GUI-mode setup, this tool scans all the files that are protected by the WFP, as well as the catalog files, to ensure that they have not been modified by external programs. If any catalog files have been modified of damaged, the WFP replaces them with a cached version from the cache folder.

User authentication, especially passwords

Windows XP is built off of a Windows 2000 base, this is why there are a few similar user authentication features (informIT, 2004). Windows XP is better than Windows 2000 in the sense that is goes further than original Windows NT 4.0. Following is a list of the biggest changes made to the management and authentication process as part of windows XP:

Everyone Group: In the past the Anonymous Group was given access to any resources that the Everyone Group had access to, but now by default the Everyone Group does not include the Anonymous group.

Guest Account: Windows XP by default lets someone that is not logged in to a domain is logged in as guest only. Users are forced to use the guest account as authentication if they want to access resources on the computer.

Service Accounts: New services have been added to Windows XP that enhances granularity of service account access. LocalService that are used to run services locally and NetworkService for running services on a network.

Blank Passwords: Users that are not part of a domain are blocked from logging in if they have blank passwords. This helps with preventing unauthorised users from accessing home workstations that are connected to the internet. Blank passwords are only allowed for local logins.

Password Reset Wizard: Windows XP has a recovery system that lets people reset their password if they forgot it. The feature uses a disk to reset a local password, this can not be done for a domain password. The disk is connected to a specific computer and can not be used on another computer, even if the username and password are identical.

Stored Usernames: Windows XP allows users to frequently store username and passwords that they use to access resources on the computer, for example a secure web site or other computers in an untrusted domain. This information is part of the user's personal profile and can be used to travel around on different networks.

Policy, trust, and assurance

Local Group Policy

In the Windows XP environment, group policies can only be inherited from the site domain to the organizational unit (Timmons). This ensures granular control to enterprise administrators. Groups and users that are part of the organizational unit will only be able to receive the settings that the administrator gives them. The User configuration policy of Windows XP has greatly expanded since NT 4.0, as it has expanded to much that it will take a whole book to write down every part of it (Timmons).

Trust and assurance

Trust is the desire or belief that the operating system will do whatever it takes to protect the resources of your computer from malicious activity. To make sure that the operating system is trustworthy, you focus on the metrics and methodologies that allows you to measure how confident you are to place that operating system in an environment and still consider that as your best option.

An example of assurance techniques is the use of analysis, formal methods for design, testing and development methodology. These techniques are categorized as either formal, semiformal, or informal.

Windows XP was seen as a trusted system because it has shown that it meets the well-defined requirements under the evaluation of a credible body of experts, that was certified to assign it a trusted rating.

Open-source software/operating systems

Software

Open-source software introduces software security vulnerabilities in any type of source code (CIPOT, 2020). Some vulnerabilities can be used to cause harm by changing the dependencies of one of your OSS projects, with the use of your other OSS project. Some vulnerabilities are introduced by programmers while they are using open-source software to complete a functionality on one of their projects.

Because programmers do not consider security while coding, they use open-source software with the idea that it is cheap and only want the function to work. This as a big impact in the work that they submit and the project that they work on (CIPOT, 2020).

Operating systems

Android is one of the most popular open-source operating system is Android (Heath, 2019). Android is based on a modified version of Linux kernel. With open-source operating systems, a lot of people scrutinizes the code, this means that it is easier to spot security holes, malicious routines, and bugs in the operating system. This does not always work, as sometimes a serious security flaw is only spotted years after release.

There are a lot of advantages of using open-source software or open-source operating systems, one being that it is free and that there is a big community of users. As with any other software, it is difficult to spot security flows and no system is completely secure.

Conclusion

This report covered the protection of Windows XP as well as some security information in other windows operating systems. The security concerns in open-source software and operating systems were addressed as well as how they contributed in terms of improving operating system security by having a community to help with spotting critical security holes and bugs.

References

Bagwe, S. (2016). *Various ways of memory and address protection.* https://www.ques10.com/p/3569/various-ways-of-memory-and-address-protection-1/

BrainKart. (2019). *Separation/Isolation*. https://www.brainkart.com/article/Separation-Isolation_9629/

CIPOT, B. (2020). The Risks and Potential Impacts Associated with Open Source. https://devops.com/the-risks-and-potential-impacts-associated-with-open-source/#:~:text=As%20open%20source%20is%20software,has%20on%20other%20OSS%20projects.

Goretsky, A. (2014). WINDOWS XP SECURITY. https://www.welivesecurity.com/wp-content/uploads/2018/03/WindowsXP_Security.pdf

Heath, N. (2019). What are open-source operating systems? Everything you need to know. https://www.zdnet.com/article/what-are-open-source-operating-systems-everything-you-need-to-know/

informIT. (2004). *Secure Authentication Features in Windows XP*. https://www.informit.com/articles/article.aspx?p=349040

Microsoft. (2020). *Description of the Windows File Protection feature*. https://support.microsoft.com/en-us/topic/description-of-the-windows-file-protection-feature-db28f515-6512-63d1-6178-982ed2022ffb

Staff, E. (2006). *Security Considerations for Embedded Operating Systems*. https://www.embedded.com/security-considerations-for-embedded-operating-systems/

Timmons, D. Windows XP Local Group Policy. http://www.trcb.com/computers-and-technology/windows-xp/windows-xp-local-group-policy-1419.htm